# §5.4 Konstruktionen mit Zirkel und Lineal

Notation. Ist $K$ ein Körper und $a \in K$, so bezeichne $\sqrt{a}$ stets eines der höchstens zwei Elemente $b \in \overline{K}$ mit $b^2 = a$

Notation. Ist $K$ ein Körper und $a \in K$, so bezeichne $\sqrt{a}$ stets eines der höchstens zwei Elemente $b \in \overline{K}$ mit $b^2 = a$ (ist $a \in \mathbb{R}_{\geq 0}$, so sei wie üblich $\sqrt{a} \geq 0$).

Notation. Ist $K$ ein Körper und $a \in K$, so bezeichne $\sqrt{a}$ stets eines der höchstens zwei Elemente $b \in \overline{K}$ mit $b^2 = a$ (ist $a \in \mathbb{R}_{\geq 0}$, so sei wie üblich $\sqrt{a} \geq 0$). Man beachte, dass $\sqrt{a}$ bis auf das Vorzeichen eindeutig bestimmt ist.

Notation. Ist $K$ ein Körper und $a \in K$, so bezeichne $\sqrt{a}$ stets eines der höchstens zwei Elemente $b \in \overline{K}$ mit $b^2 = a$ (ist $a \in \mathbb{R}_{\geq 0}$, so sei wie üblich $\sqrt{a} \geq 0$). Man beachte, dass $\sqrt{a}$ bis auf das Vorzeichen eindeutig bestimmt ist. Insbesondere ist $K(\sqrt{a})$ der Zerfällungskörper von $X^2 - a$ über $K$.

Notation. Ist $K$ ein Körper und $a \in K$, so bezeichne $\sqrt{a}$ stets eines der höchstens zwei Elemente $b \in \overline{K}$ mit $b^2 = a$ (ist $a \in \mathbb{R}_{\geq 0}$, so sei wie üblich $\sqrt{a} \geq 0$). Man beachte, dass $\sqrt{a}$ bis auf das Vorzeichen eindeutig bestimmt ist. Insbesondere ist $K(\sqrt{a})$ der Zerfällungskörper von $X^2 - a$ über $K$.

Proposition. Sei $L|K$ eine Körpererweiterung mit $\operatorname{char} K \neq 2$. Dann

$$[L : K] \leq 2 \iff \exists a \in K : L = K(\sqrt{a}).$$

Notation. Ist $K$ ein Körper und $a \in K$, so bezeichne $\sqrt{a}$ stets eines der höchstens zwei Elemente $b \in \overline{K}$ mit $b^2 = a$ (ist $a \in \mathbb{R}_{\geq 0}$, so sei wie üblich $\sqrt{a} \geq 0$). Man beachte, dass $\sqrt{a}$ bis auf das Vorzeichen eindeutig bestimmt ist. Insbesondere ist $K(\sqrt{a})$ der Zerfällungskörper von $X^2 - a$ über $K$.

Proposition. Sei $L|K$ eine Körpererweiterung mit $\operatorname{char} K \neq 2$. Dann

$$[L : K] \leq 2 \iff \exists a \in K : L = K(\sqrt{a}).$$

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(a) $\Longrightarrow$ (c) Gelte (a).

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(a) $\Longrightarrow$ (c) Gelte (a). Dann gibt es $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in \overline{K}$ mit $a_n = a$ und $[K(a_1, \ldots, a_k) : K(a_1, \ldots, a_{k-1})] \leq 2$ für alle $k \in \{1, \ldots, n\}$.

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(a) $\Longrightarrow$ (c) Gelte (a). Dann gibt es $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in \overline{K}$ mit $a_n = a$ und $[K(a_1, \ldots, a_k) : K(a_1, \ldots, a_{k-1})] \leq 2$ für alle $k \in \{1, \ldots, n\}$. Wähle $\varphi_1, \ldots, \varphi_m \in \mathrm{Aut}(\overline{K}|K)$ derart, dass $\varphi_1(a), \ldots, \varphi_m(a)$ die verschiedenen $K$-Konjugierten von $a$ sind, wobei $\varphi_1 = id_{\overline{K}}$ sei.

□

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(a) $\Longrightarrow$ (c) Gelte (a). Dann gibt es $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in \overline{K}$ mit $a_n = a$ und $[K(a_1, \ldots, a_k) : K(a_1, \ldots, a_{k-1})] \leq 2$ für alle $k \in \{1, \ldots, n\}$. Wähle $\varphi_1, \ldots, \varphi_m \in \mathrm{Aut}(\overline{K}|K)$ derart, dass $\varphi_1(a), \ldots, \varphi_m(a)$ die verschiedenen $K$-Konjugierten von $a$ sind, wobei $\varphi_1 = id_{\overline{K}}$ sei. Dann ist $L := K(\varphi_1(a), \ldots, \varphi_m(a))$ der Zerfällungskörper von $\mathrm{irr}_K(a)$ über $K$.

□

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(a) $\Longrightarrow$ (c) Gelte (a). Dann gibt es $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in \overline{K}$ mit $a_n = a$ und $[K(a_1, \ldots, a_k) : K(a_1, \ldots, a_{k-1})] \leq 2$ für alle $k \in \{1, \ldots, n\}$. Wähle $\varphi_1, \ldots, \varphi_m \in \mathrm{Aut}(\overline{K}|K)$ derart, dass $\varphi_1(a), \ldots, \varphi_m(a)$ die verschiedenen $K$-Konjugierten von $a$ sind, wobei $\varphi_1 = id_{\overline{K}}$ sei. Dann ist $L := K(\varphi_1(a), \ldots, \varphi_m(a))$ der Zerfällungskörper von $\mathrm{irr}_K(a)$ über $K$. Nach der Gradformel reicht es zu zeigen, dass $[K(a_1, \ldots, a_n, \varphi_2(a_1), \ldots, \varphi_2(a_n), \ldots, \varphi_m(a_1), \ldots, \varphi_m(a_n)) : K]$ eine Zweierpotenz ist, was mit der Gradformel durch sukzessives Adjungieren folgt.

□

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(c) $\Longrightarrow$ (b) trivial

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(b) $\Longrightarrow$ (a) Sei $L$ ein Zwischenkörper von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(b) $\Longrightarrow$ (a) Sei $L$ ein Zwischenkörper von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist. Nach Galois gilt für die Galoisgruppe $G := \mathrm{Aut}(L|K)$, dass $\#G = [L : K]$ eine Zweierpotenz ist.

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(b) $\Longrightarrow$ (a) Sei $L$ ein Zwischenkörper von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist. Nach Galois gilt für die Galoisgruppe $G := \mathrm{Aut}(L|K)$, dass $\#G = [L : K]$ eine Zweierpotenz ist. Also ist $G$ eine 2-Gruppe und daher auflösbar.

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(b) $\Longrightarrow$ (a) Sei $L$ ein Zwischenkörper von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist. Nach Galois gilt für die Galoisgruppe $G := \mathrm{Aut}(L|K)$, dass $\#G = [L : K]$ eine Zweierpotenz ist. Also ist $G$ eine 2-Gruppe und daher auflösbar. Es gibt $n \in \mathbb{N}_0$ und Untergruppen $H_0, \ldots, H_n$ von $G$ mit $G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{1\}$ und $[H_{k-1} : H_k] = 2$ für alle $k \in \{1, \ldots, n\}$.

Proposition. Sei $K$ ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:

(a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

(b) Es gibt einen Zwischenkörper $L$ von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.

(c) Für den Zerfällungskörper $L$ des Minimalpolynoms von $a$ über $K$ ist $[L : K]$ eine Zweierpotenz.

Beweis.

(b) $\Longrightarrow$ (a) Sei $L$ ein Zwischenkörper von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist. Nach Galois gilt für die Galoisgruppe $G := \mathrm{Aut}(L|K)$, dass $\#G = [L : K]$ eine Zweierpotenz ist. Also ist $G$ eine 2-Gruppe und daher auflösbar. Es gibt $n \in \mathbb{N}_0$ und Untergruppen $H_0, \ldots, H_n$ von $G$ mit $G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{1\}$ und $[H_{k-1} : H_k] = 2$ für alle $k \in \{1, \ldots, n\}$. Setzt man $F_k := L^{H_k}$ für $k \in \{0, \ldots, n\}$, so folgt mit Galois $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Notation. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\not\triangle M$ bezeichnen wir den Körper aller aus $M$ mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Notation. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\not\triangle M$ bezeichnen wir den Körper aller aus $M$ mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:

(a) $a \in \not\triangle M$

Notation. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\not\triangle M$ bezeichnen wir den Körper aller aus $M$ mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:

(a) $a \in \not\triangle M$

(b) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\mathbb{C}|\mathbb{Q}(M \cup M^*)$ mit $\mathbb{Q}(M \cup M^*) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Notation. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\not\triangle M$ bezeichnen wir den Körper aller aus $M$ mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:

(a) $a \in \not\triangle M$

(b) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\mathbb{C}|\mathbb{Q}(M \cup M^*)$ mit $\mathbb{Q}(M \cup M^*) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Mit Hilfe der Proposition und des Satzes werden wir in der Zahlentheorie zeigen, dass die regelmässigen $p$-Ecke mit $p \in \{3, 5, 17, 257, 65537\}$ mit Zirkel und Lineal konstruierbar sind.

Notation. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\not\triangle M$ bezeichnen wir den Körper aller aus $M$ mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:

(a) $a \in \not\triangle M$

(b) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\mathbb{C}|\mathbb{Q}(M \cup M^*)$ mit $\mathbb{Q}(M \cup M^*) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Mit Hilfe der Proposition und des Satzes werden wir in der Zahlentheorie zeigen, dass die regelmässigen $p$-Ecke mit $p \in \{3, 5, 17, 257, 65537\}$ mit Zirkel und Lineal konstruierbar sind. Man vermutet, dass dies die einzigen konstruierbaren regelmäßigen $p$-Ecke mit $p \in \mathbb{P}$ sind.

Notation. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\not\curlywedge M$ bezeichnen wir den Körper aller aus $M$ mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:

(a) $a \in \not\curlywedge M$

(b) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\mathbb{C}|\mathbb{Q}(M \cup M^*)$ mit $\mathbb{Q}(M \cup M^*) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Mit Hilfe der Proposition und des Satzes werden wir in der Zahlentheorie zeigen, dass die regelmässigen $p$-Ecke mit $p \in \{3, 5, 17, 257, 65537\}$ mit Zirkel und Lineal konstruierbar sind. Man vermutet, dass dies die einzigen konstruierbaren regelmäßigen $p$-Ecke mit $p \in \mathbb{P}$ sind. Johann Gustav Hermes [*1846 †1912] hat zehn Jahre seines Lebens nur mit der expliziten Konstruktion des regelmäßigen 65537-Ecks verbracht.